Schneider Electric Security Bulletin
Intel Microarchitectural Data Sampling - (ZombieLoad)

16 May 2019

Overview

Schneider Electric is aware of a security vulnerability in a wide range of Intel CPUs that may allow information disclosure. If exploited, the Microarchitectural Data Sampling (MDS) vulnerability, also named ZombieLoad, FallOut, and RIDL, would allow a malicious user who can locally execute code on a system to collect and analyze large amounts of protected data. Schneider Electric continues to assess the MDS vulnerability impact on our offers. In the meantime, we advise customers to refer immediately to Intel's security updates webpage for further information and guidance.

Details

Desktop, laptop, and virtual computers could be affected by the MDS vulnerability.

Please refer to Intel's MDS table in the Deep Dive: CPUID Enumeration and Architectural MSRs for a list of Intel processors that might be affected by MDS. Proof of concept exploit code has already been made public by the researchers who discovered this issue.

CVE-2018-12126, CVE-2018-12130, CVE-2018-12127, CVE-2019-11091 are the official vulnerability references for the MDS vulnerabilities.

Recommended Mitigations

Please note that as of the date of this publication, it is unclear whether the initial mitigations proposed by Intel will affect systems performance. Therefore, we recommend proceeding with caution if customers decide to apply patches to critical and/or performance-constrained systems. If customers elect to apply recommended patches and/or mitigations, we strongly recommend evaluating the impact of those measures in a Test and Development environment or on an offline infrastructure.

Schneider Electric continues to monitor and track vendor research into this vulnerability to determine appropriate actions to be taken. We advise customers to refer immediately to Intel's Security Center webpage for further information and guidance:

https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00233.html

https://software.intel.com/security-software-guidance/insights/deep-dive-intel-analysis-microarchitectural-data-sampling

More References:

ZombieLoad Attack website:
https://zombieloadattack.com/

U.S. Department of Homeland Security bulletin:
https://www.us-cert.gov/ncas/current-activity/2019/05/14/Intel-Releases-Security-Updates-Mitigations-Multiple-Products

General Security Recommendations

We strongly recommend following industry cybersecurity best practices such as:

- Locate control and safety system networks and remote devices behind firewalls, and isolate them from the business network.
- Physical controls should be in place to prevent unauthorized access to the ICS and safety controllers, peripheral equipment and the ICS and safety networks.
- All controllers should reside in locked cabinets and never be left in the “Program” mode.
- All programming software should be kept in locked cabinets and should never be connected to any network other than the network for the devices that it is intended.
- All methods of mobile data exchange with the isolated network, such as CDs, USB drives, etc., should be scanned before use in the terminals or any node connected to these networks.
- Laptops that are connected to any other network besides the intended network should never be allowed to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that these networks might have vulnerabilities and therefore should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

More Information

This document is intended to help provide an overview of the identified situation and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your Schneider Electric representative or your Customer Care Center https://www.schneider-electric.com/en/work/support/contacts.jsp. These organizations will be fully aware of the situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, please visit the company's cybersecurity web page:

http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

If you require additional support, Schneider Electric Industrial Cybersecurity Services team are available to help. Please visit: https://www.schneider-electric.com/en/work/services/field-services/industrial-automation/industrial-cybersecurity/industrial-cybersecurity.jsp

Legal Disclaimer

THIS DOCUMENT IS INTENDED TO HELP PROVIDE AN OVERVIEW OF THE IDENTIFIED SITUATION AND MITIGATION ACTIONS, AND IS PROVIDED ON AN "AS-IS" BASIS AND IS NOT INTENDED AS A WARRANTY OR GUARANTEE OF ANY KIND, INCLUDING WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. THE USE OF THIS NOTIFICATION, INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED TO IT ARE AT YOUR OWN RISK. SCHNEIDER ELECTRIC RESERVES THE RIGHT TO UPDATE OR CHANGE THIS NOTIFICATION AT ANY TIME AND IN ITS SOLE DISCRETION.

About Schneider Electric

Schneider Electric is leading the Digital Transformation of Energy Management and Automation in Homes, Buildings, Data Centers, Infrastructure and Industries.

With global presence in over 100 countries, Schneider is the undisputable leader in Power Management – Medium Voltage, Low Voltage and Secure Power, and in Automation Systems. We provide integrated efficiency solutions, combining energy, automation and software.

In our global Ecosystem, we collaborate with the largest Partner, Integrator and Developer Community on our Open Platform to deliver real-time control and operational efficiency.

We believe that great people and partners make Schneider a great company and that our commitment to Innovation, Diversity and Sustainability ensures that Life Is On everywhere, for everyone and at every moment.

www.schneider-electric.com

Revision Control:

Version 1 *16 May 2019*	Original Release

Product Security Office Digitally signed by Product Security Office
Date: 2019.05.16 18:57:42 -04'00'